Click here to view PowerPoint presentation in PDF format

Distribution of Situation Awareness Data in Mobile Tactical Ad Hoc Networks Using the Fisheye Routing Technique

Katarina Persson*, Ulf Sterner, Mattias Sköld, Erika Johansson
*Swedish Defence Research Agency
Command and Control Systems
P.O. Box 1165
SE-581 11 Linköping
SWEDEN

Email: {katper, ulfst, mattias, erijo}@foi.se

ABSTRACT

A mobile ad hoc network is an important component in providing future military communication. To maintain information superiority and avoid unfortunate incidents, e.g. friendly fire, it is crucial for the network to provide a Situation Awareness (SA) service. In this paper we analyze if it is possible to combine the transmission of SA position information with the routing control traffic. We show that this can be made to work for the Fisheye State Routing (FSR) protocol, and that the military demands on position accuracy can be fulfilled for nodes connected to the network in a tactical scenario.

1 INTRODUCTION

In providing future military communication, it is essential to have a high performance mobile radio network that is independent of fixed communications infrastructure. One method for obtaining area-coverage and robustness in this type of network is to enable the nodes to relay messages, thus creating a so-called *multi-hop* network. To further improve the robustness of the network, there should be no central nodes, i.e. the network management should be distributed. Such mobile distributed multi-hop networks are usually referred to as *ad hoc* networks. It is also crucial to have a Situation Awareness (SA) service [1], i.e. to have information available regarding e.g. position, speed, and direction of movement for other nodes in the network. As an example of requirements on an SA service, demands on the position accuracy (as a function of distance from ones own node) have been generated in cooperation with military personnel.

In previous evaluations of services in military mobile ad hoc networks, it has been shown that a SA service can occupy a large part of the network capacity. We here try to reduce the traffic required for the SA service by combining it with the routing protocol. We choose to use the Fisheye State Routing (FSR) protocol [2] since this protocol ”attenuates” the routing traffic in a manner similar to the accuracy demands on position information for a SA service. We will in this paper explain how this combination can be done, what demands (if any) this imposes on the FSR parameter settings and how this will work in a tactical scenario.

The paper is organized as follows. In Section 2, we briefly present the Fisheye technique and the FSR algorithm. The SA service and the demands on position accuracy are presented in Section 3, along with a description of how to combine the transmission of SA information with the routing control traffic. We describe our scenario and simulation setup in Section 4. The results from our simulations as well as from theoretical calculations are presented in Section 5. Finally, we make our concluding remarks in Section 6.

Persson, K.; Sterner, U.; Sköld, M.; Johansson, E. (2006) Distribution of Situation Awareness Data in Mobile Tactical Ad Hoc Networks Using the Fisheye Routing Technique. In *Military Communications* (pp. P13-1 – P13-10). Meeting Proceedings RTO-MP-IST-054, Poster 13. Neuilly-sur-Seine, France: RTO. Available from: http://www.rto.nato.int/abstracts.asp.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE **DEC 2006**	2. REPORT TYPE **N/A**	3. DATES COVERED **-**

4. TITLE AND SUBTITLE **Distribution of Situation Awareness Data in Mobile Tactical Ad Hoc Networks Using the Fisheye Routing Technique**	5a. CONTRACT NUMBER
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Swedish Defence Research Agency Command and Control Systems P.O. Box 1165 SE-581 11 Linköping SWEDEN**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR’S ACRONYM(S)
	11. SPONSOR/MONITOR’S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
See also ADM202750. RTO-MP-IST-054, Military Communications (Les communications militaires), The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**UU**	**10**	

2 THE FISHEYE TECHNIQUE

The Fisheye State Routing protocol [2, 3, 4] for wireless ad hoc networks is a proactive link state protocol where the objective is to keep the control traffic low and still be able to provide accurate information about the routes. The FSR protocol uses the Fisheye technique. According to this technique, a node's perception of its surroundings is similar to that of a fisheye, where the level of detail is high near the ”focal point” and decreases with the distance from the focal point. This means that when a user packet is sent, the intermediate nodes will have increasingly better routing information available as the packet approaches its destination and will use this to gradually improve the route.

Each node running FSR has to maintain a neighbor list, a topology table, and a routing table. In the topology table, information about all destinations in the network is stored. Each entry in the topology table consists of a destination, its sequence number and a list of all neighbors to this destination. The entry also contains a flag for “Need To Send”, (NTS). This flag is set, for example, when new information is added to the list entry and means that the node should send this entry to its neighbors. The topology table is continuously updated through update messages sent from neighbors. To obtain lower levels of overhead traffic in a mobile network, the generation of update messages is instead of event-driven periodic.

To generate the nodes' perception of their surroundings, each node divides the network into a number of *scopes*. For a certain node ***A***, a scope is defined as the set of destinations that it can reach within a given interval of hops. The number of scopes used to cover the network, and how they are chosen, i.e. how their borders are chosen, differs, and is not specified in [2]. An example where three scopes are used is shown in Figure 1. Here, the scopes are defined so that they contain nodes one hop away, two hops away, and three hops away, respectively.

To each scope *i*, a period T_s^i is assigned which decides how often node ***A*** may transmit information about the nodes in scope *i* to its neighbors. We define the period T_s^i as

$$T_s^i = \delta \cdot scope\ update\ factor = \delta \cdot \mathrm{round}\left(h^{\alpha}\right), \qquad (1)$$

where δ is the minimum time between two updates, *h* is the distance in number of hops to the nodes in this scope, and α determines the grade of attenuation in the network. The node however only includes information about a specific node if that node's NTS flag is set. See [4] for further details.

A node also updates its own sequence number and sets the NTS flag for its own entry in the topology table with a periodicity

$$T_u = n \cdot \delta\,, \qquad (2)$$

where *n* is a parameter we can change to improve the performance of the algorithm and δ is the minimum time between two updates, see [4]. This is done whether any of the node's neighbors have changed or no.

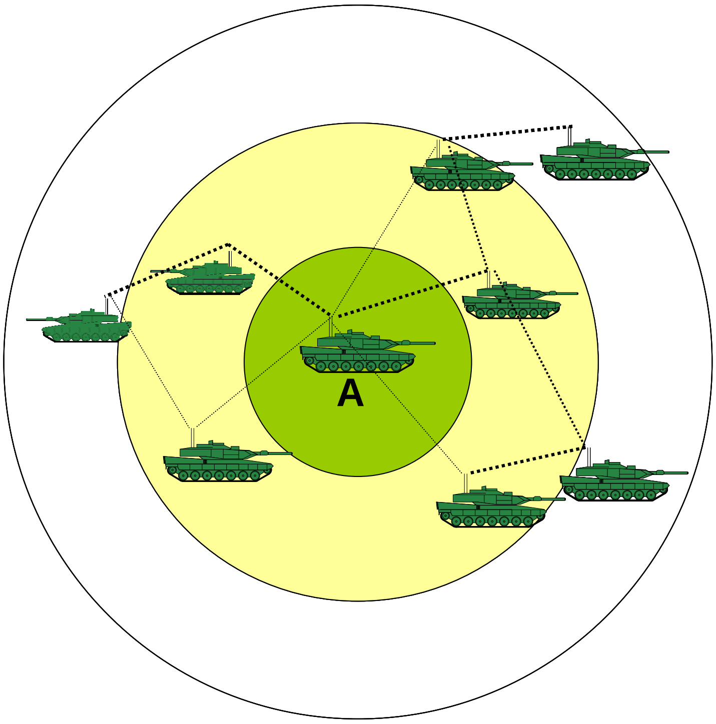

Figure 1 Every node in the network divides its possible destinations into different scopes. In this example the network is represented the way node *A* experiences it and consists of three scopes.

3 SITUATION AWARENESS (SA) SERVICE

As mentioned before, a situation awareness service will most likely be required in future military networks. As an example of demands on this service, we here present user requirements in respect to position information accuracy. These requirements originate from scenarios developed by, or in cooperation with, military personnel [1, 5]. The demand we will use throughout this paper is as follows: a node with a maximum speed of 70 km/h should not have more than one second old information about nodes *within a 3 km radius* and no more than 10 seconds old information about nodes *within a 10 km radius* [1].

3.1 Using Routing Traffic for Distribution of SA Information

One method for distributing SA information is to attach the SA data to all outgoing packets. Another method would be to attach the SA data to only some of the transmitted packets. But which ones? User traffic can be sporadic, both as to when it is generated and to whom it is transmitted. It can thus not be used since there is no guarantee that the SA data will reach all concerned nodes.

When using a proactive routing protocol, such as Fisheye State Routing (FSR), the nodes continuously try to uphold routes to one another. This means that periodically there will be routing control traffic flowing through the network. An efficient method of distributing SA data might thus be to ”piggyback” the SA data onto existing control traffic. Another advantage of this is that the update messages already contain the node identities. If the routing algorithm and the SA service could exchange information, that would further improve the combination. The routing algorithm could, for example, use the positions and velocities of other nodes to predict route changes.

The amount and instances of routing control traffic varies, however, due for example to the movements of the node. In a stationary network, where routes have been established, control traffic is only generated by the updates each node transmits about itself to its neighbors with period T_u. The information is then propagated throughout the network, eventually reaching all nodes, see [3]. These updates are the only packets that are transmitted no matter what. Hence, they are the ideal candidates for piggybacking SA data onto. This, however, imposes the SA update demands on the FSR protocol, i.e. only some FSR parameter choices will result in the fulfillment of a given set of SA demands.

3.2 How Old is the SA Information?

It is not enough to send SA information to immediate neighbors. Nodes further away are also likely to require the information. It is therefore necessary to calculate the delivery time of an update packet (with SA data attached) to any given node in the network, i.e. the time it takes for an update packet to transverse different distances. Using the ”worst case” approach, the delivery time T_D of an update packet to a node at distance *h* hops can be calculated as

$$T_D(1,\alpha,\delta) = T_{delay}$$

$$T_D(h,\alpha,\delta) = h \cdot T_{delay} + \delta \sum_{k=2}^{h} (k-1)^{\alpha} \qquad \forall h \geq 2 \qquad (3)$$

where the FSR parameters *α* and *δ* are defined in Section II. The total ”worst case” delay T_{delay} before the receiving unit gets the packet, once the FSR algorithm has determined that it is its turn for (re)transmission, is calculated as

$$T_{delay} = T_{transm} + T_{MAC} + T_{queue} \qquad (4)$$

where T_{transm} is the time it takes to transmit a message one hop, T_{queue} is the time spent in queue at the node, and T_{MAC} is the maximum delay at a node until the MAC (Multiple Access Control) protocol allows the node to transmit. Once the update packet reaches a node, it will take another T_u seconds before a new update packet arrives. The SA information, regarding a certain node, will thus be

$$T_{SA}(h,\alpha,\delta,n) = T_D(h,\alpha,\delta) + T_u \qquad \forall h, \qquad (5)$$

seconds old when the update is received. We can then, given the number of hops necessary to transverse 3 km and 10 km respectively, compare this with the demands above. We must thus choose the FSR parameters *α*, *δ*, and *n* so that we fulfill

$$T_{SA}(h,\alpha,\delta,n) \leq T_{demand} \qquad \forall h, \qquad (6)$$

if we want to meet the SA requirements.

4 SCENARIO AND SIMULATION

We consider a tactical scenario, which treat a Swedish mechanized battalion and is drawn up for armed combat on Swedish ground. The scenario work has been done together with military personnel [5]. The task for the mechanized battalion is to strike out a hostile air-landing within an area assigned to the battalion, and be prepared to strike out such an air-landing in adjacent areas. First the unit is spread out and grouped within the main anticipated drop zone. Thereafter, the anticipated air drop is found out to take place in an adjacent area. This leads to a high speed movement of the combat vehicles (speed of up to 20 m/s) on roads to the air-landing zone 10-20 km away. Nodal movements were estimated for every second of the simulation and nodal positions were located on a digitized terrain database.

The battalion consists of one type of communication platform only, a vehicle. Furthermore, we assume that the battalion consists of 6 companies, four tank companies each with 24 vehicles, one command and artillery company with 22 vehicles, and one pioneer (or support) company with 39 vehicles. Altogether, we then have 157 vehicles, or communication nodes.

4.1 Simulation

The nodes are assumed to communicate by radio and support multi-hop packet delivery. The radio network is also assumed to be decentralized, i.e. all nodes are equal, thus increasing robustness. Nodes can join or leave the network. The path loss have been calculated using our ground wave propagation library DetVag-90® [6], which takes the real terrain heights and terrain types into account. The path-loss data are calculated for the 300 MHz frequency band and the nodes are assumed to use 3 meter high antennas. Furthermore, all nodes use the same transmission power, and we have assumed that no congestion and no packet loss take place in the network. We also assume a Medium Access Control (MAC) protocol that allows each node to transmit 10 times/second. The transmitted packet is assumed to be big enough to hold the routing update information that is in turn for transmission.

5 RESULTS

We will here present our results. We begin with the number of hops needed to reach 3 and 10 km. We will then continue with the FSR parameter settings that theoretically fulfill our SA demands. We then show the accessibility to accurate position information resulting from simulations of some of these parameter settings. Finally, we present how the parameter settings affect the network.

5.1 Number of Hops Needed to Reach 3 and 10 km

To be able to determine if we fulfill the demands for the SA service we need to calculate the number of hops needed to reach nodes within a distance of 3 km and 10 km respectively. We start by simulating a large number of possible positions for the vehicles in a mechanized battalion. We calculate the network topology using DetVag-90® [6]. It can here be noted that approximately 20 % of the nodes are within 3 km from each other, and that another 60 % are 3-10 km away.

Furthermore, we cannot require the SA demands to be fulfilled for 100 % of the nodes since some of the simulated networks are not fully connected. For the nodes that are connected to the network we need on average 2.01 hops to reach the nodes within 3 km and 4.38 hops to reach the nodes within 10 km.

5.2 Parameter settings that fulfill the SA demands

Given the assumptions in Section 4 and the number of hops needed to reach 3 km and 10 km, we can calculate the FSR parameter settings that will fulfill the demand of Equation (6) by using Equation (5). We can in these equations use $T_{delay} \approx T_{MAC}$, based upon the assumptions and the distances in question. The resulting parameter settings are displayed in Table 1.

δ	*n*	α
0.1	1-6	0-3.3
0.2	1-2	0-2.7
0.3	1	0-2.4

Table 1 FSR parameter settings that will fulfill our demands on position accuracy (for the given scenario).

In Figure 2 we can see how the SA information ages with the number of hops from the origin of the information for a couple of parameter settings. Our demand is shown in the figure as a solid black curve. The top two parameter settings, shown in Figure 2 as asterisks and circles, fulfill our demands according to Table 1.

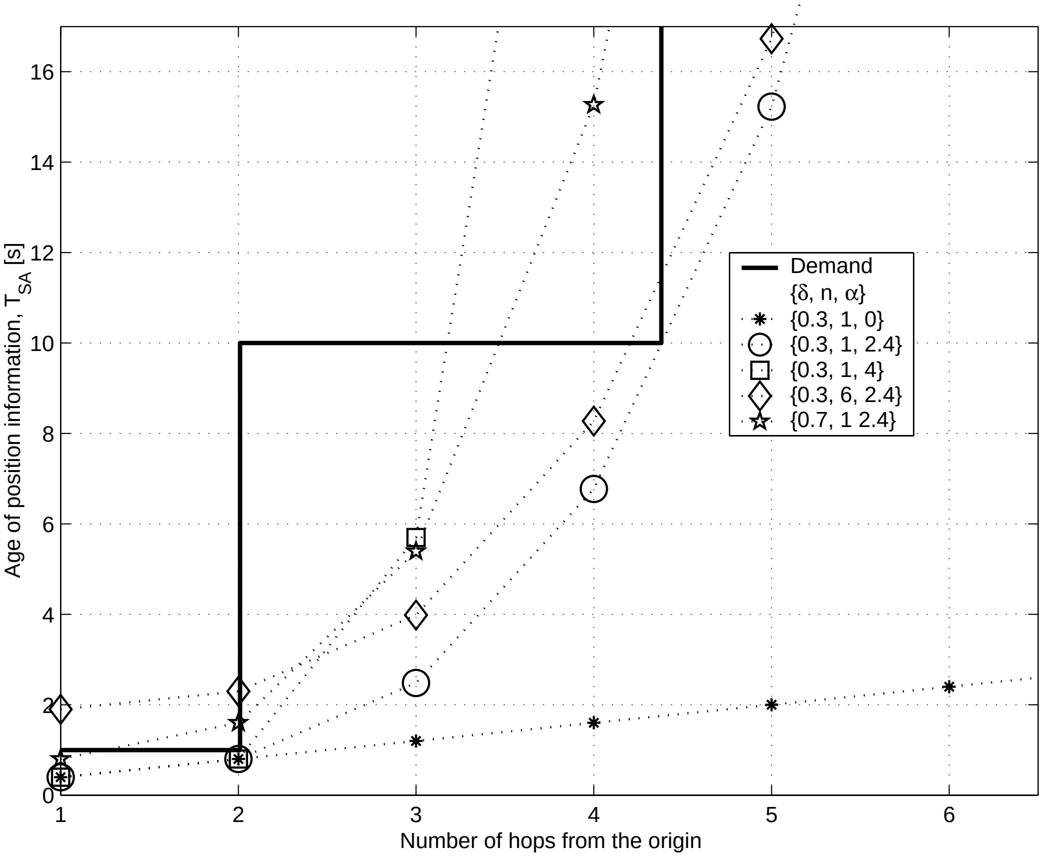

Figure 2 Demands on updates for position information (solid, black curve) and some examples of the position information ageing resulting from different FSR parameter settings

In the next parameter setting, the value of *α* is above the allowed interval. We can see from the squares shown in Figure 2 that this results in a highly exponential aging of the position information (due to waiting at intermediate nodes for the right scopes turn to transmit), thus failing to meet our demand for nodes within 10 km. An example of what happens if we instead increase *n* can be seen in the figure as diamonds. This shows that a large value of *n* can result in that update messages are generated too seldom and thereby the information is old even after one or two hops. Finally the result of using a large value of *δ* is shown in the figure as stars. This generates larger delays in the intermediate nodes and hence the position information ages rapidly.

5.3 Accessibility to SA Information in a Tactical Scenario

In Section 5.2 we have seen that there theoretically exist parameter settings for which we can fulfill the SA demand in Section 3. The question however remains, would this work in a real network?

We have thus simulated the tactical scenario from Section 4 while using the FSR protocol with position information ”piggybacked” onto the update packets. The resulting accessibility to position information that fulfills the demands on accuracy is shown in Figure 3 and 4 for nodes within 3 km and 10 km respectively. The solid and dash-dotted curves represent parameter settings that, according to our theoretical calculations, will fulfill the demands. The dashed and dotted curves represents parameter settings where the parameter α and δ respectively is to large to fulfill the demands. These curves accordingly show lower accessibility to accurate position information.

We can however also see in Figure 3 and 4 that even when using parameter settings that should fulfill our demands, the accessibility is not 100 %. This is due to the fact that the network is not fully connected at all times, for example at $t \approx 200$ and $t \approx 450$, the network is split causing many unreachable nodes and hence much inaccurate position information. On the other hand, it can be noted that, since the theoretical calculations were ”worst-case”, there are parameter settings not present in Table 1 that in a real scenario generates decent position accuracy.

Furthermore, how the parameter α is chosen, mostly affects the accessibility to accurate position information over greater distances, see the dashed and dash-dotted curves in Figure 4 and compare with Figure 3. In the same manner, the accessibility to accurate information over short distances is mostly dependant on the parameters n and δ. This is in accordance with the results shown in Figure 2 and with Equation 5.

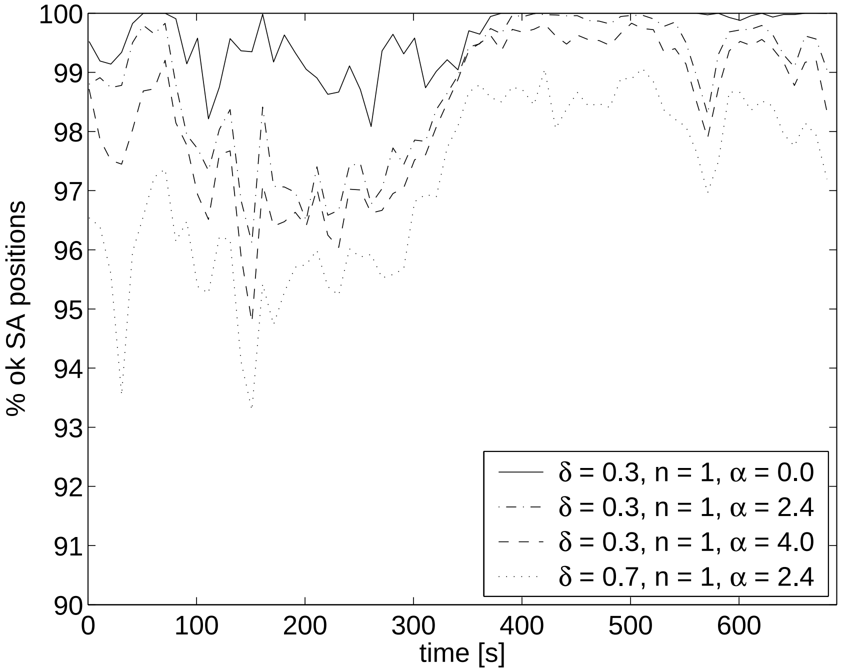

Figure 3 Accessibility to accurate position information, regarding nodes 0-3.0 km away.

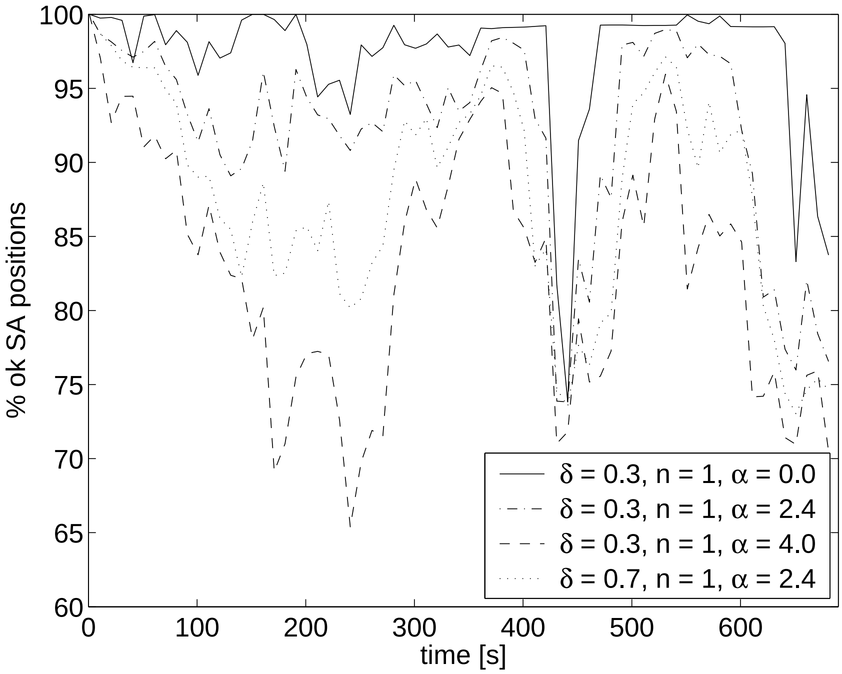

Figure 4 Accessibility to accurate position information, regarding nodes 3.0-10.0 km away.

5.4 Effects on the Network

To get high accessibility to accurate position information, we want to use small values for the FSR parameters α, n, and δ. We can see in Section 2 that this results in frequent updates and hence quite large amounts of routing control traffic, especially the parameter δ has a great impact [3]. On the other hand, parameter settings with these characteristics generally results in very good routes [3]. The optimal parameter settings for a specific network, when trying to minimize the routing traffic as well as getting routes close to the optimal ones, is however strongly connected to the minimum network capacity available [3, 4].

6 CONCLUSION

We can from our simulations conclude that it is possible to combine the distribution of SA information with FSR control traffic while meeting military demands on position accuracy. This approach increases the size of the routing control packages but results in no extra packages being transmitted for the SA service. Further gains can probably be achieved if the routing protocol and the SA service may exchange data.

It is important to choose FSR parameter settings wisely, since this has a major part in determining the performance of the SA service. Given a specific set of demands, the valid parameter settings can be calculated using the ”worst-case” approach. When used in a tactical scenario these settings results in good accessibility to accurate position information.

We can also from our results conclude that, in our scenario, the demand for nodes within 3 km was most difficult to meet and, if it is loosened a bit, many more valid parameter settings can be found.

REFERENCES

[1] M. Sköld and U. Sterner, “Evaluation of Tactical Radio Networks –Simulation Method and Results,” Command and Control Systems, FOI, Swedish Defence Research Agency, FOI memo 01-1486/L, june 2001.

[2] G. Pei, M. Gerla, and T.-W. Chen, “Fisheye State Routing in Mobile Ad Hoc Networks,” *Workshop on Wireless Networks and Mobile Computin*g, pp. D71–D78, 2000.

[3] K. Persson, M. Sköld, E. Johansson, and U. Sterner, “The Fisheye Routing Technique in Highly Mobile Ad Hoc Networks,” Division of Command and Control Systems, FOI, Swedish Defence Research Agency, Tech. Rep. FOI-R–1058–SE, December. 2003.

[4] E. Johansson, K. Persson, M. Sköld, and U. Sterner, “An Analysis of the Fisheye Routing Technique in Highly Mobile Ad Hoc Networks,” in *Proc. IEEE VTC Spring ’200*4, Milano, May 2004.

[5] F. Eklöf and B. Johansson, “Positionsförmedlingstjänst för mekaniserade förband,” Div. of Command and Control Systems Warfare Technology, FOI, Swedish Defence Research Agency, Tech. Rep. FOA-R–00-01734- 504–SE, dec 2000, in Swedish.

[6] B. Asp, G. Eriksson, and P. Holm, “Detvag-90® — Final Report,” Defence Research Est., Div. of Command and Control Warfare Technology, Linköping, Sweden, Scientific Report FOA-R–97-00566-504–SE, Sept. 1997.